



(12)

DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : 95400037.8

(51) Int. Cl.⁶ : G07F 7/10, G06F 13/38

(22) Date de dépôt : 09.01.95

(30) Priorité : 10.01.94 FR 9400164

(43) Date de publication de la demande :
12.07.95 Bulletin 95/28

(64) Etats contractants désignés :
DE GB

(71) Demandeur : FRANCE TELECOM
6, Place d'Alleray
F-75015 Paris (FR)

(71) Demandeur : LA POSTE
4, Quai du Point du Jour
F-92777 Boulogne Billancourt Cédex (FR)

(72) Inventeur : Remery, Patrick
8, Avenue de la 1ère Armée Française
F-14000 Caen (FR)
Inventeur : Darvour, Bernard
11, Allée Baudelaire
F-14000 Caen (FR)
Inventeur : Vallee, Françoise
48, rue Fleurie
F-14480 Lantheuil (FR)

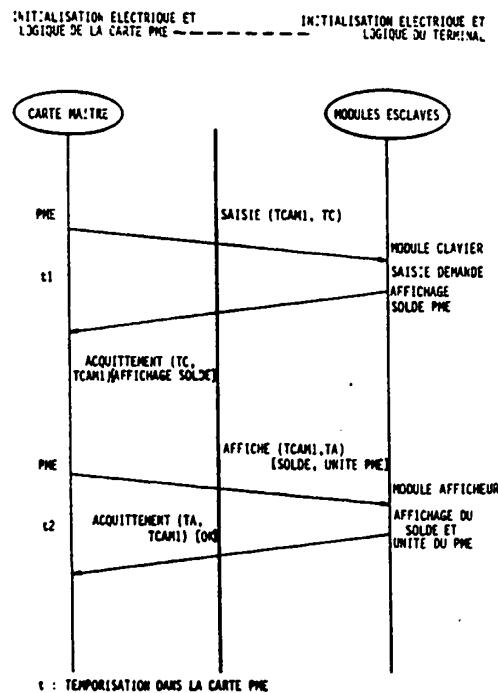
(74) Mandataire : Dubois-Chabert, Guy et al
Société de Protection des Inventions
25, rue de Ponthieu
F-75008 Paris (FR)

(54) Système pour transactions comprenant des terminaux et des cartes à mémoire et carte à mémoire correspondante.

(57) Système pour transactions comprenant des terminaux et des cartes à mémoire et carte à mémoire correspondante.

Les moyens de commande de l'exécution de la transaction sont disposés dans les cartes et non dans les terminaux, qui ne comprennent plus que des moyens esclaves.

Application au paiement électronique, au contrôle d'accès, etc...



EP 0 662 674 A1

D main t chniqu

La présente invention a pour objet un système pour transactions comprenant des terminaux et de cartes à mémoire. Elle trouve de multiples applications dans le contrôle d'accès, les transactions monétaires, le paiement par porte-monnaie électronique, etc.

Etat de la technique antérieure

Les systèmes à terminaux et à cartes à mémoire sont aujourd'hui largement répandus. Dans de tels systèmes, c'est le terminal qui gère la transaction, la carte n'étant qu'un moyen sécurisé intervenant, à la demande du terminal, pour remplir certaines fonctions. Il peut s'agir de l'identification du porteur (contrôle d'un code confidentiel), du calcul de certificats permettant d'authentifier le compte du porteur et d'autoriser des échanges de données, etc... En d'autres termes, dans l'ensemble terminal-carte, c'est le terminal qui est le maître et c'est la carte qui est l'esclave.

Le programme applicatif, qui détermine la transaction à exécuter, est placé dans le terminal. Il est écrit en général dans une mémoire morte (ou "ROM" pour "Read-Only-Memory") et ne peut être modifié. Eventuellement, il pourrait être décrit dans une mémoire vive ou à accès direct ("RAM" pour "Random-Access-Memory"). Dans ce cas, il pourrait être modifié. Mais cela supposerait que le terminal soit relié à un réseau de télécommunications approprié apte à effectuer un téléchargement au moment de la nouvelle transaction à exécuter.

Dans la plupart des systèmes actuels, les systèmes de transactions à terminaux et à cartes à mémoire sont dédiés à une application particulière, sans qu'il soit possible de modifier aisément cette application ou d'en ajouter d'autres. Par ailleurs, il est difficile et coûteux d'adapter les terminaux existants aux progrès permanents et rapides obtenus sur les cartes à mémoire.

La présente invention a justement pour but de remédier à ces inconvénients.

Le document WO-A-88 01818 décrit un système de transaction comprenant un terminal et la carte à microprocesseur d'un utilisateur. La carte comprend un mémoire EPROM, mémoire non volatile et non réinscriptible, dans laquelle une zone jeton est définie. Le document décrit les fonctions de chaque élément du système et leur interaction. En fait, il décrit un mode de paiement "off-line" basé sur l'écriture de jetons dans une carte à mémoire prépayée. L'échange de mots cryptés entre la carte de l'utilisateur et le module sécurisé à microprocesseur situé dans le terminal, autorise la délivrance d'une prestation comme l'impression d'un timbre postal.

Il est précisé que c'est le terminal qui contrôle l'in-

terface avec la carte et les opérations des différentes parties du terminal incluant le clavier, l'afficheur, l'imprimante de la machine à affranchir

Le document US-A-5 036 461 décrit un terminal dans lequel le code du programme applicatif qui sera exécuté par le terminal est enregistré dans une carte à mémoire émise par une institution financière. Lorsque la carte est insérée dans le terminal, le programme de contrôle du terminal, à l'aide d'une procédure sécurisée, lit le code écrit dans la mémoire de la carte. Le code lu est ensuite exécuté par le terminal. Cependant, la lecture sécurisée peut être coûteuse en temps d'exécution, en particulier s'il s'agit d'une application de contrôle d'accès aux transports publics, autoroutes, etc...

Exposé de l'invention

À cette fin, l'invention propose un système qui est toujours composé de transactions comprenant des terminaux et de cartes à mémoire, un ensemble terminal-carte contenant globalement des moyens dits "maîtres" aptes à commander une transaction particulière et des modules dits "esclaves" intervenant à la demande des moyens maîtres pour exécuter la transaction particulière, le système de l'invention étant caractérisé par le fait que les moyens maîtres sont disposés dans les cartes et les moyens esclaves dans les terminaux. On a donc renversé la hiérarchie des moyens. Il est alors beaucoup plus facile d'adapter, modifier ou d'ajouter des transactions en modifiant les cartes, les terminaux restant ce qu'ils sont.

L'invention objet de la présente demande élimine bien les inconvénients de l'art antérieur car le programme applicatif est exécuté par la carte à microprocesseur elle-même. Il n'est donc plus nécessaire de transférer vers le terminal le code applicatif. Dans la présente invention, le terminal met à disposition de la carte des fonctions élémentaires universelles (saisie clavier, affichage écran, transmission de données, etc...) qui sont appelées par la carte pendant l'exécution de son programme.

La présente invention a également pour objet une carte à mémoire destinée à un tel système. Cette carte se caractérise par le fait qu'elle comprend au moins une mémoire chargée par un logiciel propre à une transaction particulière et des moyens aptes à commander les moyens esclaves du terminal dans lequel la carte est introduite pour l'exécution de cette transaction.

Brève description des figures

- les figures 1a, 1b, 1c, 1d illustrent un premier exemple de transaction, qui est un paiement par carte porte-monnaie électronique,
- la figure 2 illustre un second exemple de transaction, qui est la lecture du solde d'une carte

porte-monnaie électronique.

Description détaillée de m d s de réalisation

Dans un mode de réalisation particulier, un terminal selon l'invention peut comprendre divers modules pris dans la liste suivante, qui n'est pas exhaustive :

- un module d'affichage, d'adresse TA ; plusieurs fonctions peuvent être remplies par un tel module, comme par exemple le format de caractère (gras, italique, souligné, etc...), le positionnement (à gauche, centré, à droite, à partir d'une adresse, sur la nième ligne, etc...) ; ce module pourra recevoir, par l'adresse correspondante, la commande "écriture" ;
- un module de saisie, qui peut être en particulier un clavier, d'adresse TC ; ce module pourra recevoir la commande "lecture" ; la saisie n'est pas nécessairement manuelle, mais peut être automatique dans une base de données ;
- un module de liaison vers l'extérieur, d'adresse TL ; il pourra recevoir la commande "lecture" (en réception) ou la commande "écriture" (en émission) ;
- un module mémoire, d'adresse TM ; ce module pourra recevoir la commande "lecture" ou "écriture" ; plusieurs sous-fonctions peuvent être définies (écriture à une adresse logique, effacement des zones mémoires, etc...) ;
- un module liaison vers une carte à mémoire dont l'adresse est notée TCAM ; ce module pourra recevoir toutes les commandes destinées à une carte à mémoire ou venant d'une autre carte à mémoire maître, et des acquittements venant d'autres modules.

Tous ces modules sont esclaves, c'est-à-dire qu'ils sont placés sous la commande de la carte ou d'une des cartes introduite(s) dans le terminal.

Les cartes possèdent, de leur côté, le logiciel applicatif et le protocole de communication leur permettant de communiquer avec n'importe quel terminal. Ce logiciel est écrit dans une mémoire à lecture seule (ROM) ou à lecture et écriture (EPROM, E²PROM).

La transaction est alors effectuée sous le contrôle de la carte et non sous celui du terminal. La carte transmet au terminal et à ses différents modules toutes les commandes nécessaires à l'exécution de la transaction. Un acquittement (c'est-à-dire une réponse) est retourné à la carte, laquelle l'analyse et décide de l'action suivante à entreprendre.

La carte à mémoire devient donc l'organe maître de la transaction. Le terminal et ses modules ne sont que des esclaves. S'il y a plusieurs cartes à mémoire introduites ou reliées à un même terminal, au début de la transaction, les cartes sont toutes provisoirement maîtres. Elles vont agir pour connaître leur mode de fonctionnement (maître ou esclave) par lecture du clavier du terminal. En fonction de la réponse

donnée par le clavier, qui définit le type de transaction choisi, une seule de ces cartes sera maître, les autres devenant esclaves.

Par exemple, s'il s'agit d'un paiement par porte-monnaie électronique (ou abrégé PME), c'est une carte dite module de sécurité ou SAM ("Security Application Module"), qui va diriger la transaction. Les deux cartes PME et SAM, au début de la transaction, vont lire sur le clavier le type de transaction sélectionné par le commerçant disposant du terminal. La carte SAM va se placer en mode maître et la carte PME en mode esclave. La carte PME se mettra en position d'attente des ordres provenant de la carte SAM.

Au cours d'une transaction, une carte maître peut éventuellement passer en mode esclave et vice versa.

Les figures annexées illustrent deux modes de mise en oeuvre d'un système conforme à l'invention.

Dans le cas des figures 1a, 1b, 1c, 1d, il s'agit d'une transaction de paiement par carte porte-monnaie électronique (PME) gérée par une carte SAM, qui est l'organe sécuritaire du commerçant. Celui-ci se crédite à chaque paiement du montant débité dans la carte PME.

La convention d'écriture pour les commandes et les acquittements mentionnés sur ces figures, est la suivante : la fonction remplie est d'abord indiquée (par exemple, "saisie", "initialisation", etc...) ; puis, entre parenthèses, on trouve l'adresse de la source puis celle du récepteur ; par exemple "(TCAM1, TC)" signifie que l'adresse de la source est "TCAM1", (c'est-à-dire que la source est une liaison vers une première carte à mémoire) et que l'adresse du récepteur est "TC", (le récepteur étant donc un clavier). Enfin, entre crochets et le cas échéant, on trouve les données liées à la commande ou à l'acquittement (par exemple "montant", "unité").

Dans le cas des figures 1a, 1b, 1c, 1d la transaction comprend les opérations suivantes :

- initialisation du terminal et des cartes "SAM" et "PME",
- saisie demande de transaction de paiement, pour la carte "SAM",
- saisie demande de transaction de paiement, pour la carte "PME",
- initialisation du "PME",
- affichage du solde du "PME",
- saisie du montant,
- affichage du montant,
- saisie de l'acceptation du client,
- débit du "PME",
- authentification du débit du PME et crédit du "SAM",
- affichage du nouveau solde du "PME",
- sauvegarde du total du "SAM" dans le terminal.

Dans le cas de la figure 2, la transaction dont il s'agit est la lecture du solde d'une carte PME.

La transaction comprend les étapes suivantes :

- initialisation du terminal et de la carte "PME".
- saisie de la demande de lecture du solde,
- commande affichage du solde.

On utilise donc les modules du terminal identifiés par les adresses "TA, TC, TCAM1" (la carte "PME").

5

Revendications

10

1. Système pour transactions comprenant des terminaux et des cartes à mémoire aptes à être introduites dans un terminal, un ensemble terminal-carte contenant, globalement, des moyens dits "maîtres" aptes à commander une transaction particulière et des moyens dits "esclaves" intervenant à la demande des moyens maîtres pour exécuter une transaction particulière, caractérisé par le fait que les moyens maîtres sont disposés dans les cartes et les moyens esclaves dans les terminaux la transaction étant alors effectuée sous le contrôle de la carte et non sous celui du terminal.

15

2. Système selon la revendication 1, caractérisé par le fait que certaines cartes sont dédiées à certaines applications et d'autres à d'autres applications, les terminaux étant tous semblables.

20

3. Système selon la revendication 1, caractérisé par le fait que les moyens esclaves contenus dans chaque terminal comprennent divers modules passifs dont un écran d'affichage, des moyens de saisie d'information, des moyens de liaisons intérieures et extérieures et au moins un lecteur de cartes à mémoire.

30

4. Carte à mémoire pour système selon l'une quelconque des revendications 1 à 3, caractérisé par le fait qu'elle comprend au moins une mémoire chargée par un logiciel propre à une transaction particulière et des moyens aptes à commander les moyens esclaves du terminal dans lequel elle est introduite pour l'exécution de cette transaction.

40

45

50

55

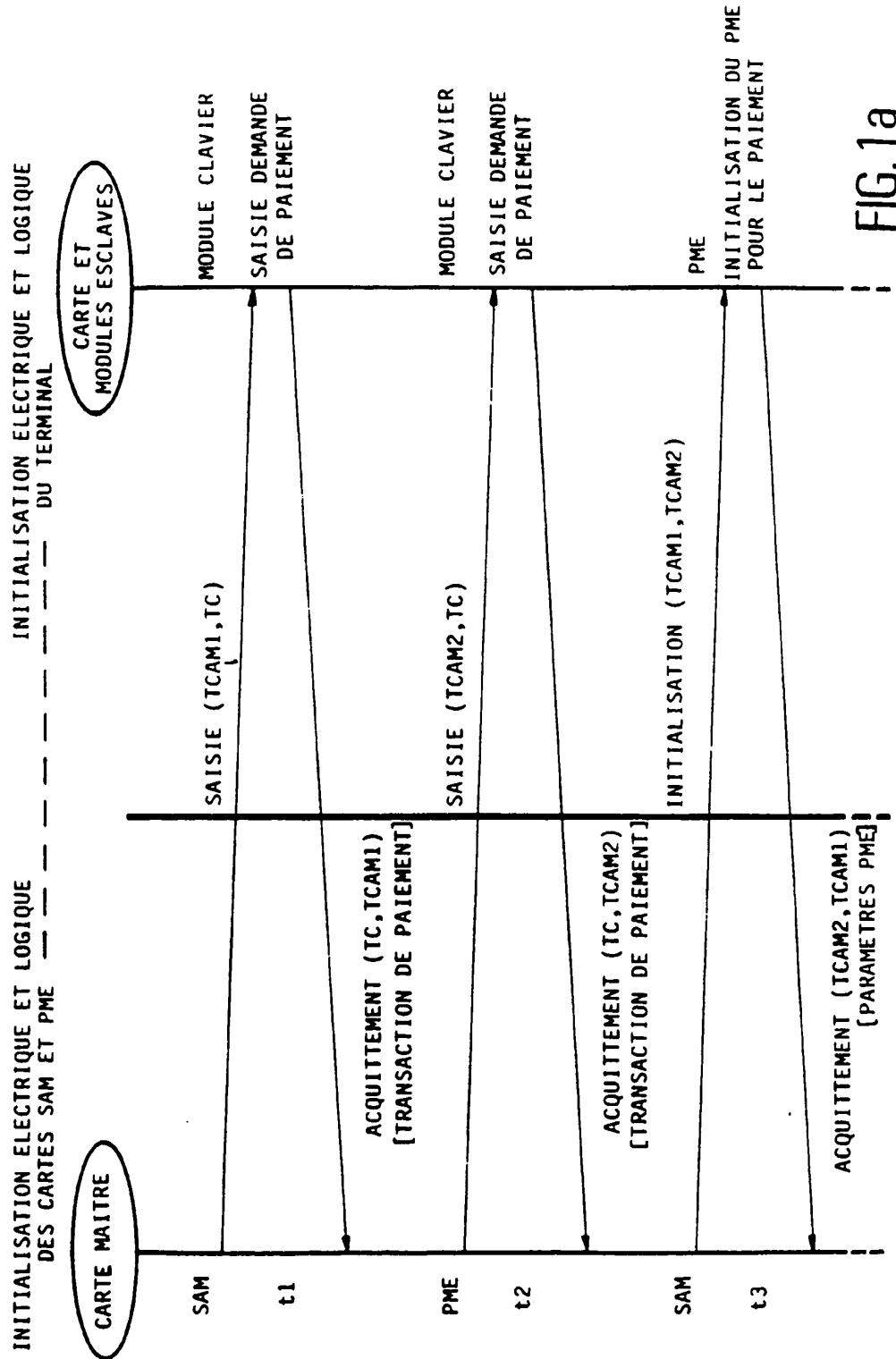
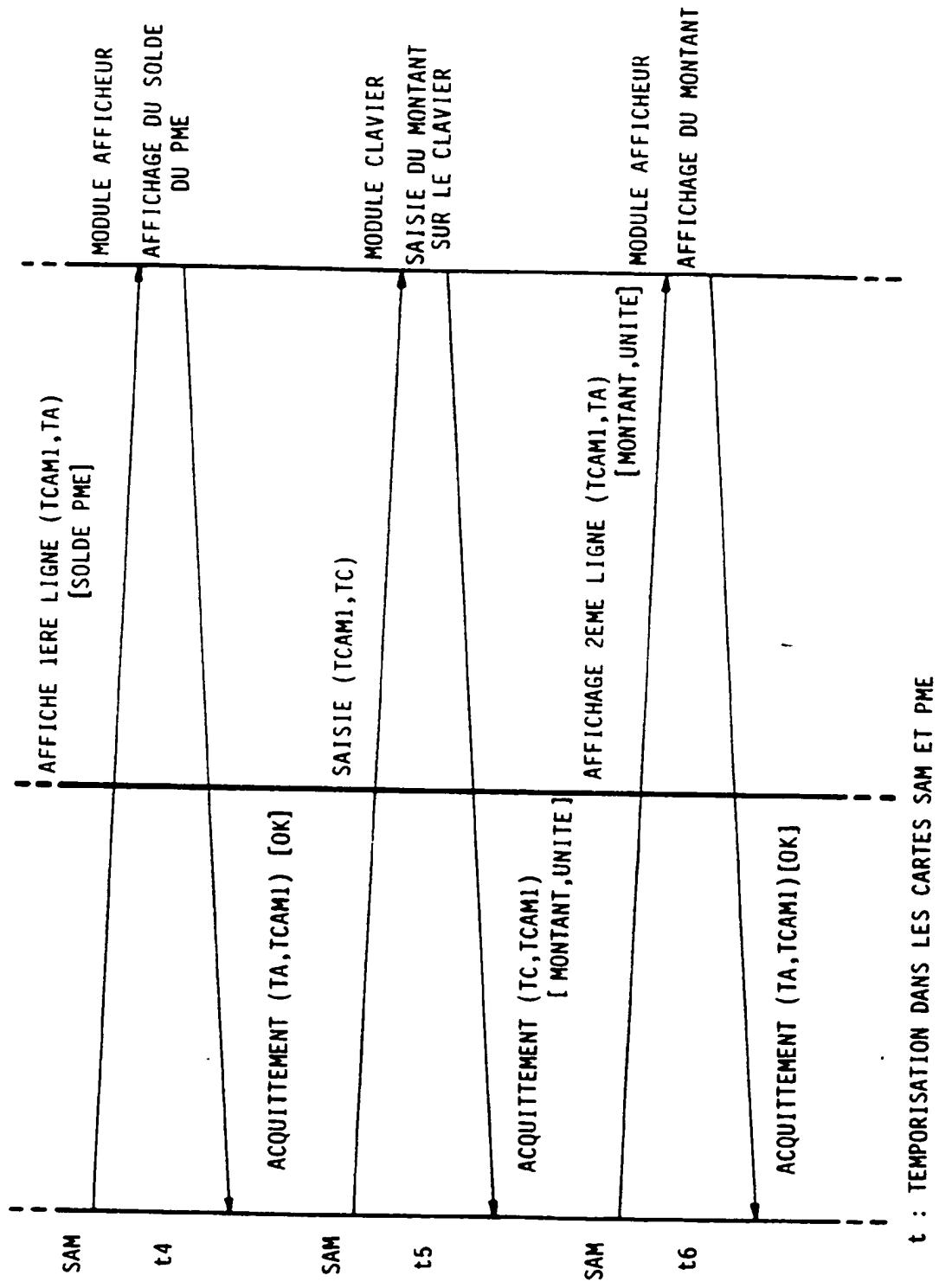


FIG. 1a



t : TEMPORISATION DANS LES CARTES SAM ET PME

FIG. 1b

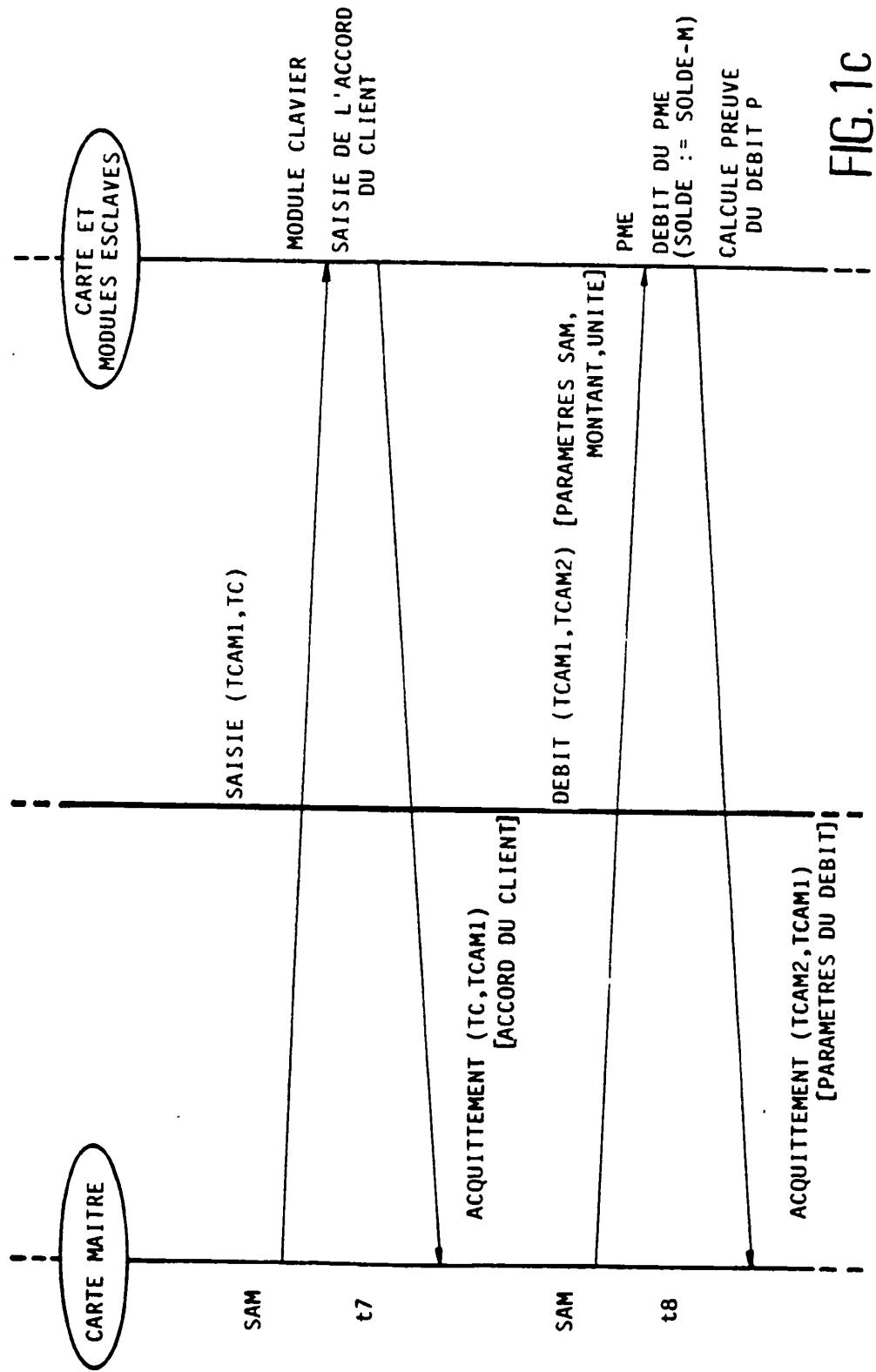


FIG. 1C

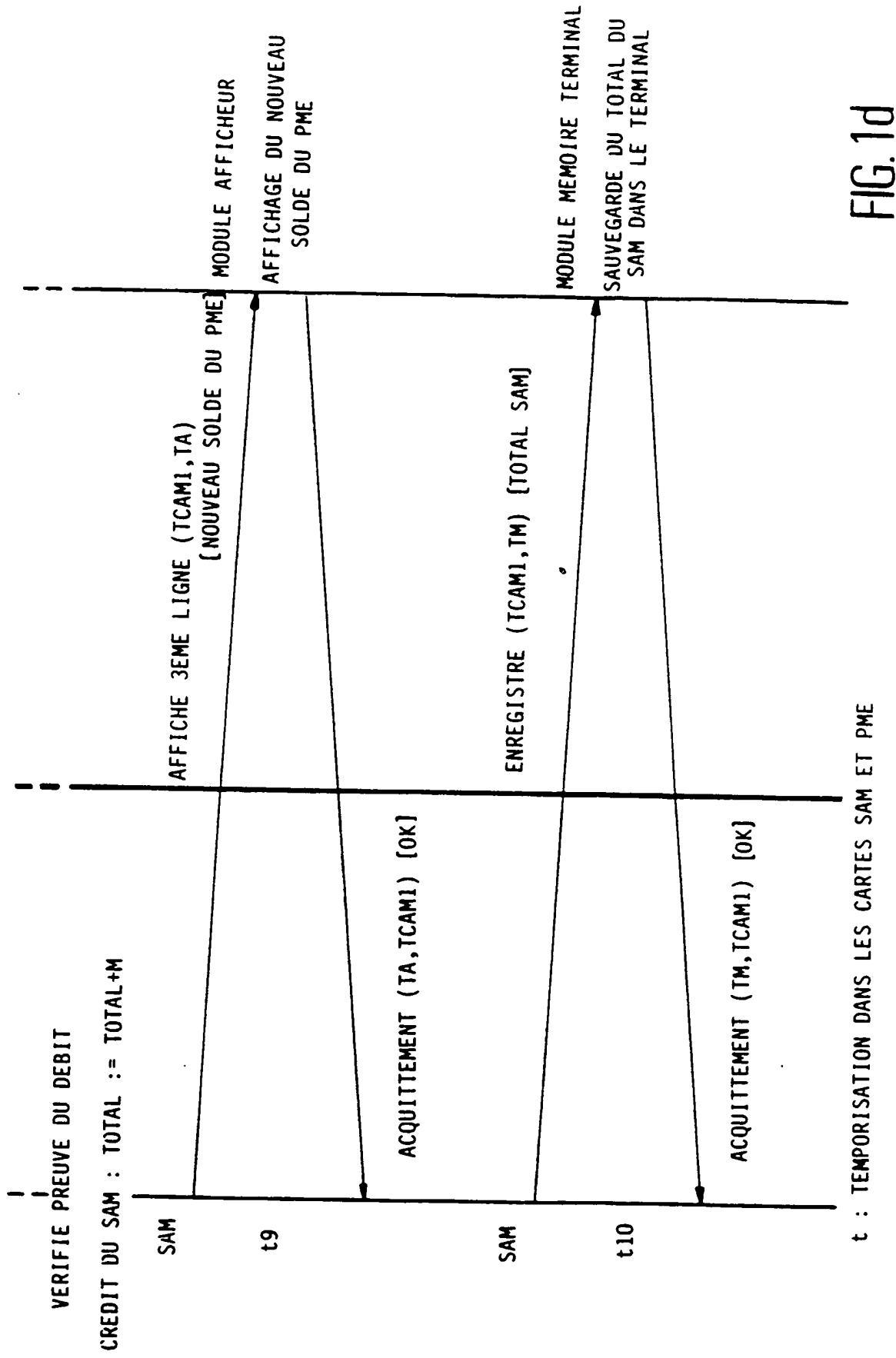


FIG. 1d

INITIALISATION ELECTRIQUE ET
LOGIQUE DE LA CARTE PME ----- INITIALISATION ELECTRIQUE ET
LOGIQUE DU TERMINAL

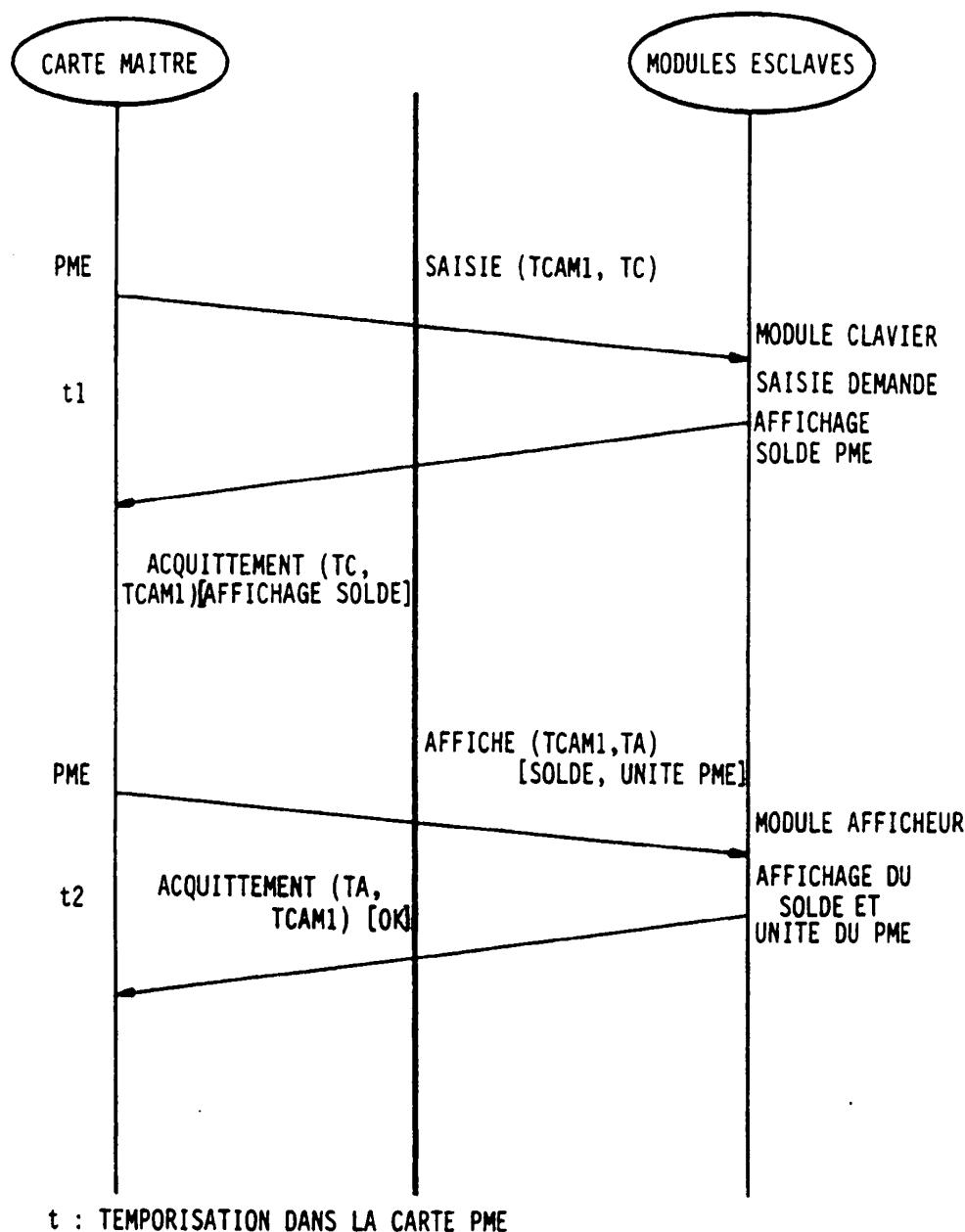


FIG. 2



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

N° de la demande
EP 95 40 0037

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.)
X	<p>WO-A-88 01818 (WRIGHT, C.) * page 1 - page 3 * * page 5 - page 7 * * page 23, alinéa 3 - page 27, alinéa 2 * * abrégé; revendications 1,2; figures 4,7-8 *</p> <p>---</p> <p>US-A-5 036 461 (ELLIOTT ET AL.) * colonne 1, ligne 13 - ligne 54 * * colonne 1, ligne 67 - colonne 2, ligne 24 * * colonne 3, ligne 45 - colonne 4, ligne 39 * * abrégé; revendications 1-3; figures 1-4</p> <p>-----</p>	1-4	G07F7/10 G06F13/38
			DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.)
			G07F G06F
<p>Le présent rapport a été établi pour toutes les revendications</p>			
Lieu de la recherche	Date d'aboutissement de la recherche	Examinateur	
LA HAYE	26 Avril 1995	NGUYEN XUAN HIEP C.	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinents à lui seul Y : particulièrement pertinents en combinaison avec un autre document de la même catégorie A : antécédents technologiques : divulgation non-série P : document breveteable		T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	